IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Case No. 1:23CR65-CMH
	)	
JAMES MEEK.	)	

DEFENDANT'S REPLY TO THE GOVERNMENT'S OPPOSTION TO HIS MOTION SUPPRESS THE EVIDENCE OBTAINED AFROM INTERNET ACCOUNTS

Defendant James Meek, through counsel, respectfully submits his reply to the government's response ("Gov't Resp." (ECF 60)) in opposition to his motion to suppress the contents of internet accounts. ECF 53.

BACKGROUND

In its response to Mr. Meek's motion to suppress the warrantless seizure of multiple internet accounts, the government concedes that it obtained the contents of three accounts that it ordered providers to preserve: two Apple iCloud accounts, and a Snapchat account. Gov't Resp. at 2.

As to the Apple account, the government obtained warrants for these accounts on November 14, 2022. But Apple was required to preserve the contents on August 26, 2022 (for [redacted]@gmail.com) and October 4, 2022 (for [redacted]@gmail.com), respectively. Accordingly, as we discussed below, in this case the two Apple accounts were seized for **106 days** and **41 days** respectively.

The government also states that while it sought preservation of the Snapchat account on October 4, 2022, "[t]he oldest content provided in response to the [November 14, 2022] search warrant was dated October 21, 2022." Gov't Resp. at 2. However, as discussed below, the fact

that the account content post-dated the preservation request does not end the issue. Rather, the question is whether the content post-dating the preservation request was nevertheless preserved as a result of the warrantless preservation directive to Snap, Inc.

ARGUMENT

I. Mr. Meek Has Standing to Seek Suppression of the Records Seized Without a Warrant.

The government argues that Mr. Meek had no reasonable expectation of privacy "in any non-content records, including subscriber information, IP addresses, or email to/from data, produced to the government." Gov't Resp. at 4. But as noted in Mr. Meek's motion, the § 2703(f) preservation letters at issue were not limited to non-content information, but the *entire contents* of Mr. Meek's internet accounts. As such, the seizures here implicated Mr. Meek's privacy interest in the contents of his accounts.

II. Preservation was a seizure, whether or not the government ultimately obtained content.

The government argues that the warrantless preservation of the accounts at issue did not violate the Fourth Amendment. These arguments are meritless.[1]

a. The private entities in this case acted as agents for the government.

The government argues that there was no Fourth Amendment violation here because the providers, which are private parties, did not act as agents of the government. Gov't Resp. at 5-6. But this argument fails as a matter of fact. The preservation orders commandeered service providers to create copies of Mr. Meek's data that were then no longer under his control. Absent

[1] The government has attempted to narrow the scope of the illegal seizures from multiple accounts by noting that it only obtained content from three of them. Gov't Resp. at 5. But whether the government obtained the content of the accounts or not, the providers in this case seized the accounts at the behest of the government by creating a copy of the contents without a warrant.

these preservation orders, these copies would not have existed. *See* Orin S. Kerr, The Fourth Amendment Limits of Internet Content Preservation, 65 St. Louis U. L.J. (2021) at 779-782 ("Content preservation in response to a § 2703(f) letter readily satisfies the Fourth Amendment test for state action. When the government makes a § 2703(f) request, the government is directly compelling the private party to act.").

The government argues that there was no agency relationship because taxpayers have a duty to maintain tax records. The government's analogy is misplaced, however, because unlike taxpayers, the service providers here had no ongoing duty to make and preserve backup copies of their customers' account in case those account are subpoenaed. Instead, the government sent the providers an order that created a duty to take a specific action at the behest of the government. 18 U.S.C. § 2703(f) ("upon the request of a governmental entity," the provider "*shall take all necessary steps* to preserve records and other evidence" in its possession, and that the records "*shall be retained* for a period of 90 days, which *shall be extended* for an additional 90-day period upon a renewed request by the governmental entity.") ((emphasis added). If one's Apple or Snapchat data were like tax records, there would have been no need for preservation orders. The fact is that there was no obligation, individually or on behalf of any service provider, to preserve Mr. Meek's data—absent the preservation orders.

The government also seeks to distinguish the cases cited by Mr. Meek that show that the government's enlistment of providers to create and preserve copies of internet accounts constitutes an agency relationship. *Commonwealth v. Gumkowski*, 167 N.E. 3d 803 (Mass. 2021); *United States v. Hardin*, 539 F.3d 404 (6th Cir. 2008). But the purported distinction—that those cases "involved more significant and invasive conduct that did result in an agency relationship"—holds no water. The test has never been the *extent* of the Fourth Amendment intrusion, but rather, the

role of the government and the intent of the party taking the action at issue. *United States v. Jarrett*, 338 F.3d 339, 345 (4th Cir. 2003) ("One highly pertinent consideration is whether the government knew of and acquiesced in the intrusive conduct and whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further her own ends"). Indeed, Courts have held that responding to search warrants is state action. *See In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197, 214 (2d Cir. 2016), *vacated as moot, United States v. Microsoft*, 138 S. Ct. 1186 (2018). Preserving the contents of accounts involves the same process as gathering the contents for production in response to a search warrant, with the primary distinction being that under 2703(f) the provider does not take the final step of sending the content to the government.

The government also relies on *California Bankers Association v. Shultz*, 416 U.S. 21 (1974), but that case does not support the government's position. Gov't Resp. at 6. *Shultz* addressed the argument made by banks that their Due Process rights were violated by the "unreasonable burdens" of certain record-keeping requirements. *Id.* at 42. The focus of the banks' argument were the unreasonable burdens placed them "by seeking to make the banks the agents of the Government in surveillance of its citizens." *Id.* at 45. But the basis of the Supreme Court's decision was not anything to do with the issue of agency, as the government suggests. Rather, it was the extent of the burdens on the banks, which the Court held were common and were far lesser burdens than other regulatory approaches that were clearly lawful. *Id.*at 50. Neither the reasoning nor the holding of *Shultz* bears on who is a Fourth Amendment state actor.

Here, by sending the preservation letters ordering the providers to seize the accounts, the "Government knew of and acquiesced in the private search," and by following the mandate of the

letter, "the private [company] intended to assist law enforcement" and "had [no] other independent motivation." *Jarrett*, 338 F.3d at 345. Under Fourth Circuit law, an agency relationship existed.

b. A preservation request fulfilled by a provider is a Fourth Amendment seizure.

The government argues that a preservation request is not a seizure because there is no "meaningful interference with an individual's possessory interest in [the] property." Gov't Resp. 7-10. This argument is easily refuted.

First, the government claims that when it ordered the providers to preserve the account information, it "obtain[ed] no information at all." *Id.* at 7. This is a distinction without a difference because, as noted above, the providers were acting as agents of the government when seizing the accounts. The conduct of the providers in this case are thus state action attributable to the government.

Second, the government claims that Mr. Meek retained control over his account. *Id.* This is clearly not true, because if Mr. Meek sought to exercise control over his account by, for example, deleting emails with a former employer or confidential journalistic source, he would not have ability to exercise such control. This is the direct result of the government's enlistment of a third party with the very purpose of depriving him of that control. The government suggests that Mr. Meek's argument is absurd because he is "essentially arguing that he should have the right to obstruct justice by deleting his data at any time." *Id.* The government's argument could just as easily apply to any illegal Fourth Amendment seizure. As Professor Kerr writes,

> the risk that valuable electronic evidence "can be deleted irretrievably in an instant" does not differentiate electronic seizures from physical seizures.272 The concern justifying temporary warrantless physical seizures has always been that a seizure now may be needed to ensure that important evidence is not lost. Recall the many cases in which the government seizes a package suspected of containing drugs.273 Unless the government held on to the package, the package and its contents could be gone forever. Drugs might

> be flushed down the toilet, moved to an unknown place, or consumed. The ease of deleting digital evidence is nothing new and does not justify a different rule.

Kerr, Content Preservation at 272-73. Just as an individual who objects to a warrantless search of his home is not arguing that he has a right to commit crimes in his home, Mr. Meek objects to the seizure of his internet accounts because the Constitution requires a warrant, and no warrant exception applies to the seizures here.

The government's arguments also contradict Supreme Court precedent. *United States v. Jacobsen* states that property is seized "when there is some meaningful interference with an individual's possessory interests in that property." 466 U.S. 109, 113 (1984). *See also United States v. Jefferson,* 571 F. Supp. 2d 696, 703 (E.D. Va. 2008) (holding that "recording . . . information by photograph or otherwise" is a seizure, "even if the document or disc is not itself seized," because "the Fourth Amendment privacy interest extends not just to the paper on which the information is written or the disc on which it is recorded but also to the information on the paper or disc itself"); *United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) (holding that the Government's retention of electronic copies of the defendant's personal computer "deprived him of exclusive control over those files," which was "a meaningful interference with [the defendant's] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment."), vacated, *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016) (*en banc*).

The fact that creating a backup copy of the accounts constitutes a seizure is also supported by the warrant process set forth in warrant process under 18 U.S.C. § 2703(a). When the government obtained the contents of internet accounts though a warrant, courts have assumed or expressly held that the duplication of the contents prior to disclosure to the government constitutes a "seizure." *Search of Info. Assoc. with [Redacted]@Mac.Com*, 25 F. Supp. 3d 1, 7 (D.D.C. 2014) (Facciola, MJ) ("Even if, as Professor Orin Kerr has stated, a search does not occur until the data

is exposed to possible human observation . . . the seizure of a potentially massive amount of data without probable cause has still occurred—and the end result is that the government has in its possession information to which it has no right."); *United States v. Bowen*, 689 F. Supp. 2d 675, 684 (S.D.N.Y. 2010) (describing the copying of account contents as a seizure).

For all of these reasons, copying Mr. Meek's internet accounts was a Fourth Amendment seizure.

c. Mr. Meek did not consent to an unlawful Fourth Amendment seizure of his accounts.

The government argues that Mr. Meek consented to the seizure of his accounts by the providers, at the behest of the government. Gov't Resp. 10-12.

The government relies on the Apple, Inc. and Snap, Inc., terms of service[2] to which Mr. Meek allegedly agreed. *Id.* at 11. As discussed in Mr. Meek's motion, terms of service do not eliminate user Fourth Amendment rights or amount to consent because they are contracts between private Internet companies and private users such Mr. Meek. The government nevertheless argues that because the agreements included provisions that authorized the providers to preserve account data where "legally required to do so" (Apple) or upon receipt of "valid legal process." (Snap). *Id.* However, even if these terms of service were ones that Mr. Meek acquiesced to simply by using the services at issue, he is not alleging that Snap or Apple breached the terms. Instead, he is alleging that the government violated the Fourth Amendment by prevailing on the providers to seize the accounts without first establishing probable cause to do so.

[2] The government presents the *current* terms of service in support of its argument—but the government has not established that these were the terms of service to which Mr. Meek allegedly agreed at the time he began using the services.

The government seeks to distinguish *United States v. Washington*, 573 F.3d 279 (6th Cir. 2009) and *Byrd v. United States*, 138 S.Ct. 1518 (2018) on the ground that "neither of those cases had the defendants expressly consented to the action in question—as the defendant had here." Gov't Resp. at 11. But contrary to the government's claim, nowhere in the terms of service does the user waive his Fourth Amendment rights, permitting the warrantless seizures of his accounts. The scenario here is therefore no different than if the government had sent the providers a fake warrant for the account contents, and the providers complied. Mr. Meek would not be arguing that providers breached the terms of service; he would be arguing that the account contents were illegally seized and searched. So here, the government violates the Fourth Amendment by ordering the contents of an account seized without a warrant, supported by probable cause. *See Soldal v. Cook Cnty., Ill.*, 506 U.S. 56, 61 (1992) (explaining that seizures must be justified under the Fourth Amendment independently of any searches).

The government also argues that the providers had "common authority" over the contents of the account, and Mr. Meek assumed the risk of providers preserving his data. This argument is without merit, because such authority is "not to be implied from the mere property interest a third party has in the property," such as Apple and Snap's ownership of the platform that hosts the account. *United States v. Matlock*, 415 U.S. 164, 172 n.7 (1974). Instead, common authority is based on "on *mutual use* of the property by persons generally having *joint access or control for most purposes*, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched." *Id.* (emphases added). The providers in this case are not co-owners of the content who have "mutual use" of the accounts, but rather bailees of the digital papers and communications therein. *See, e.g., Krupa v. TIC Int'l Corp.*, No. 1:22-

CV-01951-JRS-MG, 2023 WL 143140, at *1 (S.D. Ind. Jan. 10, 2023) (finding that company holding the plaintiff's data was a bailee of the information) (relying on *Carpenter v. United States*, 138 S. Ct. 2206, 2268–69 (2018) (Gorsuch, J., dissenting).

Furthermore, "assumption of risk" is not an independent theory on which the government can rely. Rather, it is a factor courts have relied upon in determining whether "common authority" over property exists. *Matlock*, 415 U.S. at 172 n.7; *Georgia v. Randolph*, 547 U.S. 103, 111-12 (2006); *Fernandez v. California*, 571 U.S. 292, 301 (2014). Because Snap and Apple do not have common authority over the accounts at issue, Mr. Meek did not "assume the risk" that these companies would seize the account contents on behalf of the government absent a warrant.

d. Preservation was not reasonable.

"If the defendant meets his burden of establishing a warrantless seizure, the burden then shifts. The government must establish the warrantless seizure was reasonable." *United States v. Shrum*, 908 F.3d 1219, 1229 (10th Cir. 2018). The government cannot meet that burden here.

(1) The Seizures Cannot Be Justified Based on Probable Cause.

Probable cause at the inception of a seizure permits the government to temporarily detain property pending the issuance of a warrant. *See United States v. Place,* 462 U.S. 696, 701 (1983) ("Where law enforcement authorities have probable cause to believe that a container holds contraband or evidence of a crime, but have not secured a warrant, the Court has interpreted the Amendment to permit seizure of the property, pending issuance of a warrant to examine its contents, if the exigencies of the circumstances demand it or some other recognized exception to the warrant requirement is present."). This authority allows the government to seize property based on probable cause so long as agents proceed to work diligently to obtain a warrant that permits the property's long-term seizure and subsequent search. *See id.* The preservation statute expressly

contemplates this temporary and limited role, as it limits preservation to circumstances "pending the issuance" of a warrant (for contents) or other legal process (for non-content records). 18 U.S.C. § 2703(f)(1).

The seizure of Mr. Meek's accounts cannot be justified on this basis for two reasons. First, seizure of the accounts was not based on probable cause. The temporary warrantless seizure of property must be justified "at its inception." *United States v. Sharpe*, 470 U.S. 675, 482 (1985). But the government did not have the probable cause needed to justify the preservation at its inception. As Professor Kerr has explained, "[p]reservation letters are typically submitted early in an investigation just in case probable cause eventually emerges." Orin S. Kerr, The Fourth Amendment Limits of Internet Content Preservation, 65 St. Louis U. L.J. (2021) at 766. When investigators learn a suspect has an online account, they will submit a preservation request to seize the account. *See id.* A common government strategy is to seek "unlimited preservation, just in case probable cause might emerge," *id.* at 757, in order to "ensure that every record in existence at the outset is available if probable cause later develops." *Id.* at 757. About half the time, governments do not follow up with any legal process at all, much less with a warrant needed to compel the contents of an account. *See id.* at 770.

Although this is a case when the government did follow up as to some accounts—the government eventually obtained a warrant under 18 U.S.C. § 2703(a)—a warrantless seizure must be justified "at its inception." *Sharpe*, 470 U.S. at 682. On August 26 and October 4, 2022, the dates the government directed the preservation of the accounts, the government lacked probable cause to believe the account contained evidence. The government bears the burden of establishing sufficient cause at the time of the seizure, *see id.* at 709, and it has provided no basis to conclude it can satisfy that burden.

The warrantless seizure was unreasonable for a second reason. Even assuming the government can establish probable cause at the time of preservation, the seizure was unreasonable because the government waited too long to obtain a warrant. When the government seizes property without a warrant based on probable cause, "the Fourth Amendment requires that they act *with diligence* to apply for a search warrant." *United States v. Smith*, 967 F.3d 198, 202 (2d Cir. 2020) (emphasis added). When the government fails to seek a warrant expeditiously, the warrantless seizure violates the Fourth Amendment even if a warrant is later obtained. *See id.*

United States v. Mitchell, 565 F.3d 1347 (11th Cir. 2009), provides a useful reference point. In *Mitchell*, the Eleventh Circuit ordered the suppression of a computer hard drive because investigators allowed 21 days to elapse after seizing the hard drive before they obtained a warrant. The government had validly seized the computer based on exigent circumstances, as there was probable cause to believe it contained child pornography. But the case agent then left town for two weeks of training, and he did not obtain a warrant until he returned and the computer had been seized for 21 days. *See id.* at 1349-50. In ordering suppression of the hard drive and its contents, the Eleventh Circuit held that the 21-day period was unreasonable in the absence of "compelling justification for the delay." *Id.* at 1351. The government's failure to expeditiously apply for a warrant was fatal: "No effort was made to obtain a warrant within a reasonable time because law enforcement officers simply believed that there was no rush." *Id*. at 1353.

Mitchell supports suppression in this case. As in *Mitchell*, "[n]o effort was made to obtain a warrant within a reasonable time because law enforcement officers simply believed that there was no rush." *Id*. If the 21-day delay between the initial seizure and the warrant in *Mitchell* was too long, surely the delays in this case were too long. *See also Smith*, 967 F.3d at 211 (ruling that

the Fourth Amendment was violated by a one-month delay after computer seizure before obtaining a warrant).

(2) The Seizure Cannot Be Justified By General Reasonableness Principles.

The government tries to meet its burden of justifying the seizure of Mr. Meek's accounts on general reasonableness grounds in the absence of probable cause. But the Fourth Amendment's requirements do not simply get swept aside whenever the government believes that a warrantless seizure is reasonable. Instead, this can only be based on established exceptions, which are: (a) the investigative detention principles of *Terry v. Ohio*, 368 U.S. 1 (1968); (b) the "special needs" exception; and (c) the rules for detention during the execution of search warrants. None of these lines of cases supports the government's position.

(a) Investigative Detention Doctrine Cannot Justify the Preservation. First, the preservation seizure cannot be justified by the investigative detention principles of *Terry*. It is true that *Terry*'s stop-and-frisk framework can permit a very brief investigative detention of property based only on reasonable suspicion. *See United States v. Place*, 462 U.S. 696, 707 (1983) (allowing the warrantless seizure of luggage based on reasonable suspicion that it contained narcotics). This doctrine has allowed the brief detention of postal mail in transit so drug-sniffing dogs can sniff them for drugs. *See, e.g., United States v. LaFrance*, 879 F.2d 1, 10 (1st Cir. 1989) (allowing detention of FedEx package for 135 minutes based on reasonable suspicion).

But that rule cannot justify the seizure here. A *Terry*-stop detention must be brief. The government can detain property based on reasonable suspicion only to "*quickly* confirm or dispel the authorities' suspicion." *Place*, 462 U.S. at 702 (emphasis added). The seizure can last only as long as the "the police diligently pursued a means of investigation that was likely to confirm or dispel their suspicions *quickly*." *Sharpe*, 470 U.S. at 686 (emphasis added). In *Sharpe*, for example,

the Supreme Court ruled that a 90-minute detention of luggage based only on reasonable suspicion was excessive: "The length of the detention of respondent's luggage alone precludes the conclusion that the seizure was reasonable in the absence of probable cause." *Id*. at 709.

Such a limited detention authority cannot justify the seizure of Mr. Meek's accounts for the period that they were seized in this case. That period was far too long. Further, even if *Terry* and *Place* can permit a seizure that long in theory, it could not do so here because the government did not have the required reasonable suspicion at the inception of the seizure that the seized account contained evidence.

(b) The "Special Needs" Doctrine Cannot Justify the Preservation. The seizure also cannot be justified under the "special needs" doctrine. The special needs doctrine can permit suspicionless searches and seizures "where the program was designed to serve special needs, beyond the normal need for law enforcement." *City of Indianapolis v. Edmond*, 531 U.S. 32, 37 (2000). For example, the Court has allowed some kinds of drunk-driving checkpoints when has been shown to advance a public interest in safety. *See Michigan Dept. of State Police v. Sitz*, 496 U.S. 444, 455 (1990).

The special needs doctrine does not justify preservation of Mr. Meek's accounts for two reasons. First, the preservation was not conducted for a special need beyond the normal need for law enforcement. As the United States Department of Justice itself has emphasized, the purpose of preservation under § 2703(f) is to help criminal investigators with their criminal investigations: Preservation is designed "to minimize the risk" that "evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure." U.S. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 139 (2009).

That is not a special need. Instead, it is a classic law enforcement interest in seizing evidence of crime to prevent its destruction. *See Edmond*, 531 U.S. at 48 (concluding that narcotics checkpoints cannot be justified under the special needs exception because their "primary purpose . . . is ultimately indistinguishable from the general interest in crime control"); *Ferguson v. City of Charleston*, 532 U.S. 67, 83-84 (2001) (ruling that drug testing program was not covered by the special needs doctrine because "the immediate objective of the searches was to generate evidence for law enforcement purposes").

Second, even if preservation were somehow deemed a special need (which it clearly is not), it cannot satisfy the reasonableness requirement imposed on special needs seizures. *See, e.g., Illinois v. Lidster*, 540 U.S. 419, 427-78 (2004) (considering whether a special-needs seizure was constitutionally reasonable by weighing the government interests advanced by the seizure and the citizen interests infringed by it). The preservation authority the government claims to have is astonishing. It is the power to seize any person's online account, at any time, for any reason—or even for no reason at all. In the government's view, anyone's online account—even *everyone*'s online account, as the government can preserve multiple accounts at once—can be seized entirely at the government's discretion. The limitless discretion the government claims cannot satisfy any reasonableness test.

Delaware v. Prouse, 440 U. S. 648 (1979), is instructive. In *Prouse*, the Supreme Court invalidated a program of suspicionless traffic stops to determine if drivers had a valid license and registration. *See id.* at 663. The government claimed that the discretionary stops were reasonable under the special needs doctrine because checking for license and registration advanced the public interest in traffic safety. *See id.* at 658. Although the Court agreed that traffic safety was a special need, *see id.* at 658-59, the Court ruled that such seizures without reasonable suspicion were

unreasonable. *See id.* at 659-63. "The marginal contribution to roadway safety possibly resulting from a system of spot checks cannot justify subjecting every occupant of every vehicle on the roads to a seizure—limited in magnitude compared to other intrusions but nonetheless constitutionally cognizable—at the unbridled discretion of law enforcement officials." *Id.* at 661. This was especially true because "[a]utomobile travel is a basic, pervasive, and often necessary mode of transportation," *id.* at 662, so that the power to stop cars without reasonable suspicion impacted almost everyone: The Fourth Amendment did not permit such an "evil" of "standardless and unconstrained discretion." *Id.* at 661.

The reasoning of *Prouse* is equally applicable to Internet content preservation under 18 U.S.C. § 2703(f). Modern Internet communications services and devices are "such a pervasive and insistent part of daily life" that using them is "indispensable to participation in modern society." *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018). "The marginal contribution" to Internet crime investigations "resulting from a system" of discretionary Internet preservation "cannot justify subjecting every [user] of every [service on the Internet] to a seizure—limited in magnitude compared to other intrusions but nonetheless constitutionally cognizable—at the unbridled discretion of law enforcement officials." *Prouse*, 440 U.S. at 661.

(C) Rules for Detention During the Execution of a Warrant Cannot Justify Preservation.

The government might also try to justify the suspicionless seizure of Mr. Meek's accounts under the detention principles of *Michigan v. Summers*, 452 U.S. 692 (1981). *Summers* held that officers executing a search warrant can detain persons on the premises without additional particularized suspicion. *See id.* at 701. This is justified, the Court reasoned, by the government's interest in preventing flight as well as protecting officer safety. *See id.* at 701-05.

Summers cannot justify a preservation seizure because its reasoning was expressly dependent on the government having already obtained a warrant. "Of prime importance in assessing the intrusion," the Court explained, "is the fact that the police had obtained a warrant to search respondent's house for contraband." *Id.* at 701. Detention of those on the premises was reasonable without additional cause because "[a] neutral and detached magistrate had found probable cause to believe that the law was being violated in that house and had authorized a substantial invasion of the privacy of the persons who resided there." *Id.* The warrant had to come first, and obtaining it then justified the lesser intrusion of brief detention. Establishing probable cause "sufficient to persuade a judicial officer that an invasion of the citizen's privacy is justified" made it "constitutionally reasonable to require that citizen to remain while officers of the law execute a valid warrant to search his home." *Id.* at 704-05.

The opposite happened here. The government ordered preservation just in case probable cause might eventually emerge. Warrants were obtained, but not until November 14, 2022. This case involves seizing just in case a warrant might someday be legally obtained, not seizing as part of the execution of an existing warrant. *Summers* does not apply.

III. Suppression of the illegally seized accounts is required in this case.

a. The good faith exception does not apply.

The government argues that the good faith exception should apply because, as in *Krull*, the government was relying on a statute— 18 U.S.C. § 2703(f)—in issuing the preservation letters. The government's reliance on *Illinois v. Krull*, 480 U.S. 340 (1987) is misplaced. In that case, the Supreme Court held that investigators act reasonably when they rely on "the judgement of the legislature that passed the law," even if the law is subsequently held unconstitutional. But as noted in Mr. Meek's motion to suppress, the statute at issue here does not "expressly authorize" the

actions taken by the agents because the mistake here belongs to law enforcement instead of Congress. When Congress enacted 18 U.S.C. § 2703(f), it did not make any legislative judgments about what law enforcement seizures are permitted or when they are constitutional.

The preservation statute is not directed to governments at all. The Fourth Amendment governs when a preservation request can be made, and the preservation statute does not say otherwise." Mot. To Suppress (ECF 53) at 16. Indeed, *Krull* itself left open the scenario in which police officers believe that they are reasonably interpreting a statute, but in fact are acting outside of the statute. *See Krull*, 480 U.S. at 361–62 n.17 (declining to address whether the exclusionary rule would apply if an officer acted outside a statute that authorized searches and seizures later deemed unconstitutional, and noting that the application of the exclusionary rule "might well be different when police officers act outside the scope of a statute, albeit in good faith" because "the relevant actors are not legislators or magistrates, but police officers"); *See also United States v. Wallace,* 885 F.3d 806, 811 n.3 (5th Cir. 2018) (noting, in a Fourth Amendment challenge brought to surveillance claimed to be authorized by the Stored Communications Act, that "[t]he holding of *Krull* does not extend to scenarios in which an officer erroneously, but in good faith, believes he is acting within the scope of a statute").

Next, the government argues that requiring a showing of probable cause would defeat the purpose of preservation. The government suggests that it must have the ability to seize account contents, for without it, it cannot develop probable cause. The government's argument fails as a legal matter because the Fourth Amendment requires that in order to seize property, the government must have probable cause, establish exigent circumstances, or demonstrate that some other exception applies. There is no special provision of the Fourth Amendment stating that government agents can seize the contents of an account because they have decided that it will help

their investigation. The act of preserving records does nothing to develop probable cause. This case is an apt illustration: the preservation of the internet accounts did nothing establish probable cause. Instead, it was the warrantless review of the Dropbox content (which in this case happened to be unlawful) that formed the basis of the government's warrants. Thus, it is not unreasonable to require the government to show some kind of cause (whether probable cause, or reasonable suspicion) before seizing property. The Fourth Amendment requires nothing less. Because the government has shown *no* cause in this case, the Court need not determine the specific showing that must be made before seizing internet account without a warrant.

b. The government cannot establish "inevitable discovery" as to the Apple accounts.

Finally, the government argues that the seizures at issue were not the "but-for" cause of the information that the government ultimately obtained from the providers. But the government only provides specific support for this claim as to the information obtained from Snap, Inc. It does not make the same representation regarding the content obtained from two Apple accounts, which is a burden that the government bears. *See, e.g., United States v. Lazar*, 604 F.3d 230, 239–41 (6th Cir. 2010) (holding that the government has the burden of proving inevitable discovery). Instead, the government attempts to evade this burden by shifting it to Mr. Meek. Gov't Resp. at 15 ("the defendant does not allege and cannot establish the requisite causation."). Thus, the government must show that none of the information it obtained from Apple originates from the unlawfully seized preservation copy, as opposed to the warrant copy. It has failed to do so here.

Moreover, as to the information seized from Snap, Inc., the government has not shown whether this information was independently held in the account until the time of the warrant, or if it was only held in the account as a result of the preservation letter. If the latter, then the analysis

is the same, because the fruits of the warrant are due to a warrantless seizure of the account accompanied by no showing of cause.

CONCLUSION

For all of the foregoing reasons, the Court should suppress the information preserved in Mr. Meek's internet accounts based on the government's warrantless preservation letters, and turned over to the government based on a subsequent warrant.

Respectfully Submitted,

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing document VIA ECF which provides a copy to the AUSA of record.

By: /s/ *Eugene V. Gorokhov*
Eugene Gorokhov, Bar. No. 73582
Attorney for Defendant
BURNHAM & GOROKHOV, PLLC
1750 K Street NW, Suite 300
Washington, DC 20006
(202) 386-6920 (phone)
(202) 765-2173 (fax)
eugene@burnhamgorokhov.com